

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



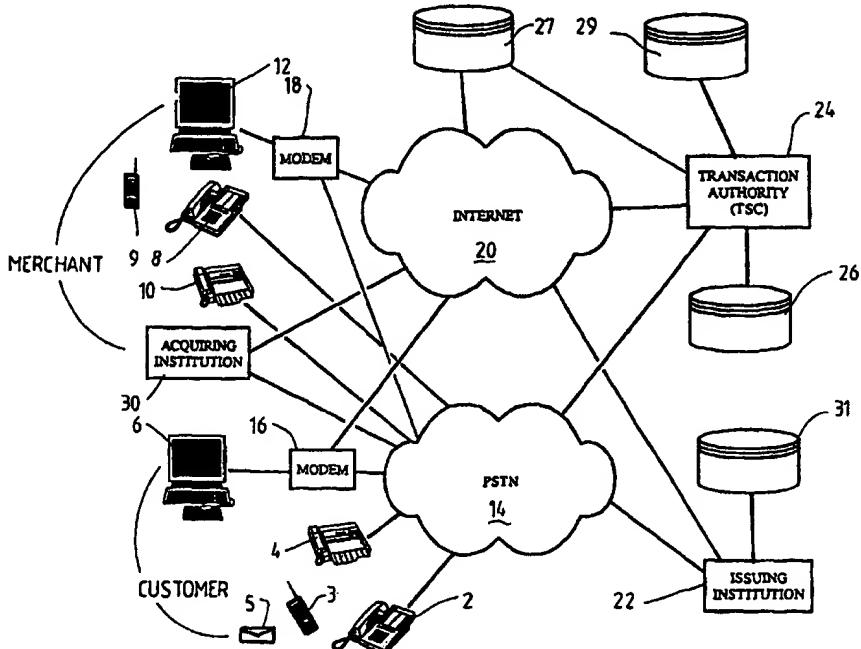
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| | | | |
|--|--|--|---|
| (51) International Patent Classification ⁶ : G06F 17/60 | | A1 | (11) International Publication Number: WO 00/02150 |
| | | | (43) International Publication Date: 13 January 2000 (13.01.00) |
| (21) International Application Number: PCT/AU99/00536 | | (81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). | |
| (22) International Filing Date: 1 July 1999 (01.07.99) | | | |
| (30) Priority Data: PP 4439 1 July 1998 (01.07.98) AU PP 5211 12 August 1998 (12.08.98) AU | | | |
| (71) Applicant (<i>for all designated States except US</i>): WEBCARD INC. [VU/VU]; 1th floor, Pentecost Vanua Building, Port Vila (VU). | | Published <i>With international search report.</i> | |
| (72) Inventor; and (75) Inventor/Applicant (<i>for US only</i>): RENARD, Julien, Gaston, Robert [AU/AU]; 125 Studley Road, Heidelberg, VIC 3084 (AU). | | | |
| (74) Agent: CARTER SMITH & BEADLE; 2 Railway Parade, P.O. Box 557, Camberwell, VIC 3124 (AU). | | | |

(54) Title: TRANSACTION AUTHORISATION METHOD

(57) Abstract

A system for conducting a remote financial transaction between a customer and a merchant wherein for each transaction a customer is issued with a transaction code by a transaction authority (24) for use as a substitute for the account number of the customer from which funds will be drawn by the merchant for the transaction. An address code is retrieved from a storage means (27) representing a delivery location for the customer to which goods and/or services provided by the merchant will be sent. Authorisation for the transaction from the customer occurs when the customer provides the merchant with the transaction code. In order for the merchant to claim funds from the customer the merchant transmits an amount together with a merchant code and the transaction code to the transaction authority (24). Upon validation by the transaction authority (24) the address code and an approval code is sent to the merchant for use in initiating the transfer of funds to the merchant account. The merchant may cross check the storage means (27) on entering the address code to obtain a corresponding physical or electronic address where the goods are to be delivered.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|----|--------------------------|----|---------------------------------------|----|---|----|--------------------------|
| AL | Albania | ES | Spain | LS | Lesotho | SI | Slovenia |
| AM | Armenia | FI | Finland | LT | Lithuania | SK | Slovakia |
| AT | Austria | FR | France | LU | Luxembourg | SN | Senegal |
| AU | Australia | GA | Gabon | LV | Latvia | SZ | Swaziland |
| AZ | Azerbaijan | GB | United Kingdom | MC | Monaco | TD | Chad |
| BA | Bosnia and Herzegovina | GE | Georgia | MD | Republic of Moldova | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagascar | TJ | Tajikistan |
| BE | Belgium | GN | Guinea | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan |
| BF | Burkina Faso | GR | Greece | ML | Mali | TR | Turkey |
| BG | Bulgaria | HU | Hungary | MN | Mongolia | TT | Trinidad and Tobago |
| BJ | Benin | IE | Ireland | MR | Mauritania | UA | Ukraine |
| BR | Brazil | IL | Israel | MW | Malawi | UG | Uganda |
| BY | Belarus | IS | Iceland | MX | Mexico | US | United States of America |
| CA | Canada | IT | Italy | NE | Niger | UZ | Uzbekistan |
| CF | Central African Republic | JP | Japan | NL | Netherlands | VN | Viet Nam |
| CG | Congo | KE | Kenya | NO | Norway | YU | Yugoslavia |
| CH | Switzerland | KG | Kyrgyzstan | NZ | New Zealand | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | Democratic People's Republic of Korea | PL | Poland | | |
| CM | Cameroon | KR | Republic of Korea | PT | Portugal | | |
| CN | China | KZ | Kazakhstan | RO | Romania | | |
| CU | Cuba | LC | Saint Lucia | RU | Russian Federation | | |
| CZ | Czech Republic | LI | Liechtenstein | SD | Sudan | | |
| DE | Germany | LK | Sri Lanka | SE | Sweden | | |
| DK | Denmark | LR | Liberia | SG | Singapore | | |
| EE | Estonia | | | | | | |

TRANSACTION AUTHORISATION METHOD

The present invention relates to a system and method of conducting a transaction between a customer and a merchant located remotely from each other. The present invention also relates to a method of validating a financial transaction between a customer and a merchant. The present invention further provides a method for ensuring the delivery of goods or services to the correct address of the customer.

To perform transactions without exchanging money or cash, a customer uses a credit card or debit card or the like to provide funds to the merchant for the transaction. Where the customer requires to initiate and complete a transaction remotely, for example, over the Internet or by telephone or by post, the customer is required to provide to the merchant their credit card number and its expiry date. These details may be transmitted across insecure channels, particularly over the Internet which is an open communications network, where a third party may be able to access or alter the data in transit and fraudulently use the credit card number and expiry date for subsequent transactions for some time without the knowledge of the customer or cardholder. Furthermore, unscrupulous merchants may store or hold credit card information for fraudulent use at a later time or this information may be stolen and used by criminals to make fraudulent purchases.

Generally the merchant will access a database of known credit card numbers that are to be refused approval for transactions for one reason or another. Provided the credit card number is a valid number and is not on that database, the merchant will obtain authorisation of the transaction and deliver the goods to the address specified by the customer without actually receiving funds from the customer's bank into the merchant's bank account. Such a transfer of funds is generally performed after the goods have been distributed to the customer. Therefore there is much emphasis or onus placed on the merchant to actually obtain the funds from the customer. There is no guarantee that the funds transfer will actually take place in situations where the customer for one reason or another is not able to pay for the goods and the account holder may repudiate or veto the payment, possibly long after the original transaction and long after the goods or

services have been delivered by the merchant thus presenting the merchant with the possibility that they will not receive the funds for the transaction.

Currently there exists a large number of potential or actual customers who refrain from conducting a transaction over an open network using their credit card 5 details due to the perceived or apparent insecurities of such a network. Various encryption technologies have been or are proposed to be implemented to enable secure electronic transactions to take place over communication networks. For example, for transactions conducted over the Internet, a public key cryptographic system has been provided using the secure socket layer (SSL) protocol developed 10 by Netscape Communications. This protocol provides data encryption, server authentication, message integrity and optionally client authentication for a transmission control protocol/Internet protocol (TCP/IP) connection. However, the procedure for enabling transactions to take place securely over open networks implementing SSLs between all parties involved in the transaction is rather 15 cumbersome, demands a level of knowledge and understanding of the encryption process and security issues by all parties which may be excessive and is considered to be particularly onerous for merchants and their customers. Some banks and credit card organisations have also proposed schemes such as the SET scheme which requires the customer to maintain and understand security software on their 20 computer and will require upgrading with each successive generation of computer operating system. Such encrypted systems rely essentially for their security on the encryption of all transmissions and, as such, any improvements in computer speeds or decryption technologies present a threat to the security of such transmissions and are likely to require constant upgrading of encryption technologies.

25 The present invention desirably provides a system and method for conducting a transaction which does not require complex encryption technologies, requires the customer or account holder to be responsible for approving the transaction, requires a pre-arranged delivery address to be supplied by the customer and, most importantly, does not require the customer to transmit their 30 card number or account information across an open and unsecured communications channel. Furthermore, the present invention desirably ensures delivery of goods and/or services to the correct address of the customer and SUBSTITUTE SHEET (Rule 26) (RO/AU)

payment of funds from the correct account to the account of the intended merchant when the transaction is conducted using a communications network.

According to a first aspect of the invention there is provided a method of conducting a financial transaction between a customer and a merchant, wherein 5 said customer is remotely located from said merchant and said customer having an account associated with a credit card or debit card or the like from which funds for said transaction will be drawn by said merchant, said merchant having a Merchant Code for use in said transaction, the method comprising the steps of:

10 providing a Transaction Code to said customer for use in said transaction as a substitute for the account number of said customer;

establishing an Address Code for said customer that represents a delivery location for goods and/or services provided by said merchant to said customer;

15 wherein in order to authorise said transaction, said customer provides said merchant said Transaction Code such that the account number of said customer is not disclosed to said merchant.

The method may include linking the Address Code to a physical address location. The Address Code may also be linked to an electronic address that is mapped to a physical address location.

According to a second aspect there is provided a method of validating a 20 financial transaction between a customer and a merchant, where said customer is remote from said merchant, said method comprising the steps of:

establishing an Address Code for said customer, said Address Code representing a delivery location for goods and/or services provided by said merchant to said customer;

25 matching said Address Code to a physical address of said customer;

providing a data storage means for storing said Address Code and associated physical address;

30 wherein use of said Address Code in said financial transaction ensures that delivery of said goods and/or services is to the address nominated by said customer and thereby validates said transaction.

The method may include linking the Address Code to an electronic address mapped to the physical address in situations where goods and/or services are

transmitted electronically to the customer. The customer may request a Transaction Code for use in the transaction as a substitute for a number of an account of the customer from which funds are drawn by the merchant.

According to a third aspect of the invention there is provided a system for 5 conducting a financial transaction between a customer and a merchant, wherein said customer is remotely located from said merchant and said customer having an account associated with a credit card or debit card or the like from which funds for said transaction will be drawn by said merchant, said merchant having a Merchant Code for use in said transaction, the system comprising:

10 a first storage means for storing a Transaction Code for use in said transaction, said Transaction Code being a substitute for the number of said account of said customer;

means for transmitting said Transaction Code to said customer in response to a request by said customer for approval for said transaction; and

15 a second storage means for storing an Address Code, said Address Code being linked to a delivery location nominated by said customer where goods and/or services provided by said merchant as part of said transaction are to be delivered;

20 wherein in order to authorise said transaction, said customer provides said merchant said Transaction Code such that said account number of said customer is not disclosed to said merchant.

The delivery location may be a physical address or an electronic address mapped to a physical address.

According to a fourth aspect of the invention there is provided a method of ensuring correct delivery of goods and/or services to a customer from a merchant 25 as a result of a remote transaction between said customer and said merchant, said method comprising the steps of:

establishing a storage means for storing one or more Address Codes, wherein each stored Address Code represents a delivery location for receipt of said goods and/or services;

30 matching said Address Codes to respective physical addresses in said storage means; and

accessing said storage means in order to retrieve a corresponding delivery

location on entering an Address Code, or in order to retrieve an Address Code corresponding to an entered delivery location.

The invention will hereinafter be described in a preferred embodiment, by way of example only, with reference to the drawings wherein:

5 Figure 1 is a block diagram of a system used for conducting a financial transaction between a customer and a merchant in accordance with the invention;

Figure 2 is a flow diagram depicting the process of a customer seeking remote transaction facilities; and

10 Figure 3 is a flow diagram depicting the process involved in conducting a transaction and the merchant making a claim for payment in accordance with the invention.

Figures 4(a), 4(b) and 4(c) are schematic diagrams showing examples of the contents of a second storage means in accordance with the present invention;

15 Figure 5 is a schematic diagram of the contents of an Issuer database; Figure 6 is a schematic diagram of the contents of a database controlled by a Transaction Authority or an Issuer; and

Figure 7 is a schematic diagram of the contents of a customer database.

When a customer desires to make remote transactions using their credit card or debit card, or any other type of card or storage device or account number which 20 enables funds to be transferred from a customer's account to a merchant's account, the customer applies to their Issuing Institution or card issuing organisation (either or both hereinafter referred to as "Issuer") for remote transaction facilities. The merchant's account may be held by an Acquiring Institution (hereinafter referred to as "Acquirer") which may be a bank or other financial institution making remote 25 transaction facilities available to merchants wishing to make sales to customers located remotely from the merchant and accepting funds from a customer's account for deposit to the merchant's account. The Issuer may be a bank or other financial institution making remote transaction services available to a customer via an account held by the customer at the Issuer and making transfers of funds at the 30 request of the customer from the customer's account to a merchant's account. The Issuer may have access to a Transaction Authority (hereinafter referred to as a Transaction Services Centre (TSC)). The TSC may be an organisation or group of
SUBSTITUTE SHEET (RULE 26) (RO/AU)

organisations entrusted by Issuers and Acquirers with the information necessary to approve transactions and route requests regarding transactions to the appropriate financial institutions. On receipt of a customer request for remote transaction facilities, the Issuer will go through the necessary checks to enable such facilities, 5 including rigorous identification of the customer, and then issues to, or obtains from, the customer a password or other identifying information, such as a pass phrase, PIN, number, code, or biometric data ("Passcode") that is known only to the customer and to the Issuer, for use when communicating with the Issuer. The Passcode may be used by an Issuer to authenticate the identity of a customer 10 requesting a Transaction Code (to be described hereinafter) for a remote transaction. The procedures to be followed and identification to be used will typically vary from Issuer to Issuer and the modes of communication agreed between customer and Issuer will typically also vary to suit local conditions and banking, legal or social requirements.

15 The customer also provides to the Issuer at least one physical address, and, if desired, an electronic address with a corresponding physical address. This address will be used as a delivery location for delivery of goods or services by merchants. Referring to Figure 1, the physical address, including the physical address associated with the electronic address where applicable, will be converted 20 into a unique numerical Address Code which is stored by the Issuer in a database 31 and is supplied to, or may already be known to the customer from a second storage means 27 storing Address Codes and matching them to delivery locations nominated by the customer. Where more than one delivery address is nominated by the customer a method of referring to the corresponding Address Code stored 25 by the Issuer without explicitly stating the Address Code (for example by index number) may be agreed to enhance the security of subsequent communications by obviating the need to explicitly state Address Codes.

30 The customer is then equipped to initiate remote transactions, that is transactions not involving the physical presence of a card or the customer. When wishing to make a transaction to purchase goods or services from a merchant, the customer will usually contact that merchant by post, e-mail, facsimile, telephone or through the Internet. A customer may use either the post 5, or their telephone 2, ~~SUBSTITUTE SHEET (RULE 26) (RO/AU)~~

facsimile machine 4 or personal computer (PC) 6 to communicate with the merchant's telephone 8, facsimile 10 or PC 12 respectively. The customer may use a communications network such as Public Switched Telephone Network (PSTN) 14 when contacting the merchant by either telephone or facsimile or 5 electronic mail. In situations where a mobile telephone 3 is used, a corresponding mobile telecommunications network may be used. The merchant may be contactable through mobile telephone 9. Electronic mail may be transmitted between the customer's personal computer 6 via modem 16 over the PSTN 14 or Internet 20 and through modem 18 of the merchant and direct to the merchant's PC 10 12. Alternatively, the customer may communicate with the merchant over the Internet 20 through their respective PCs 6 and 12 and respective modems 16 and 18 or through any other channel which is or will become available and is 15 considered suitable for such communication.

While communicating with the merchant, the customer will obtain an 15 approximate price for the goods and/or services they require from the merchant together with a Merchant Code identifying the merchant. Every merchant participating in remote transactions will have a Merchant Code which is a publicly advertised number which may be assigned by a financial institution, such as the Acquirer, providing the remote transaction facilities to the merchant. This code 20 could in principle be the existing merchant number as currently used for credit card transactions, however, an Address Code belonging to the merchant may be registered for use as the Merchant Code.

The customer will then contact their Issuer 22 usually by the telephone 2, facsimile 4, through the Internet 20, or even by using an automatic teller machine 25 (ATM) and the customer will supply to the Issuer 22 the following information:

- (a) their credit or debit card or account number, or an agreed reference thereto;
- (b) the Merchant Code;
- (c) the Limit Amount for the transaction; which is an amount of money 30 for a transaction which may not be exceeded for that transaction;
- (d) the Passcode, and optionally;
- (e) an Address Code, corresponding to the desired delivery location, or

an agreed reference to an Address Code, if the customer has previously registered with the Issuer more than one Address Code.

The items of information in (a), (d) and (e) may be conveniently stored in an Issuer database 31, an example of which is shown in Figure 5. It is to be noted 5 that multiple Address Codes 32 may have been supplied by the customer when applying for the facility and in such case one will need to be selected, either explicitly or by reference. Details on the customer account status and balance are also stored in the database 31. The database 31 is maintained by the Issuer in a secure and private manner.

10 The use of an Address Code belonging to the customer and corresponding to a pre-arranged delivery address (goods or services will be delivered only to the legitimate address of the customer) has the effect of making the system secure such that there is no essential requirement to encrypt information sent to the Issuer by the customer over an open channel, such as the Internet. However, if desired, the 15 customer when communicating with the Issuer via the Internet 20 may use an encryption protocol such as the SSL so that any account information or Passcode transmitted from the customer to the Issuer is secure. To reduce inconvenience to the customer, when using their PC the process could be quite transparent to the customer by using appropriate software in conjunction with the browser that the 20 customer is using for the World Wide Web of the Internet. To make this communication even more secure, a range of Passcodes could be used to cater for different methods of customer to Issuer communications. In addition, if the customer is communicating with the Issuer by telephone or electronically, instead of the Issuer requesting the entire Passcode from the customer, they may request 25 only certain digits or characters out of the full digit string of the Passcode. Furthermore, the particular digits requested out of the string may be determined by a randomising function of the Issuer's computer system so that the same digits are not requested by the Issuer on each occasion that a Transaction Code is requested by the customer. By way of simplified example, the Issuer may on one occasion 30 request only five out of sixteen digits that make up the entire Passcode, requesting the third, fourth, eighth, thirteenth and fifteenth digits and on another occasion may request six digits, say the first, third, fourth, sixth, ninth and twelfth digits for

another Transaction Code request. This would make it difficult for any eavesdropper to intercept the entire Passcode as they would be required to track a large number of request calls made between the customer and the Issuer in order to complete the entire Passcode and would not in fact know when such information 5 was complete. The use of Address Codes ensuring delivery only to the legitimate address of the customer in any case renders these additional security features optional rather than essential to the integrity of the system.

The Transaction Code may be a number assigned by a TSC on request from a customer relayed by an Issuer, relating to a particular transaction between a 10 merchant holding a valid Merchant Code and a customer having an account with an Issuer, and relating to a particular Address Code representing a delivery address for the customer and a particular amount or Limit Amount.

Once the Issuer is in receipt of this information (a to e above) it will then check the available credit, or funds, and status of the card or account, verify the 15 Passcode, verify the Address Code and check the Merchant Code for validity through one or more TSCs 24. The TSCs may also have information stored in a database 26 relating to the available credit and status of the card or account together with other identifying information about the customer and selected merchant for a transaction. This information together with the Merchant Code 20 may be transmitted from the TSCs 24 to the Issuer 22 over the PSTN 14 or by proprietary protocols internal to the Issuer and TSCs as currently used or that may be used in the future.

The Address Code, as mentioned previously, is uniquely linked to a corresponding physical address, or an electronic address mapped to a physical 25 address which uniquely identifies the location to which the goods or services will be delivered. Address Codes may be stored in a second storage means, such as a database 27 accessed publicly through the Internet 20. The Address Code is a numerical code explicitly identifying a particular delivery location on the Earth, derivable by mathematical calculation from survey data and published when 30 activated in the publicly readable database 27 which is securely maintained by, for example the Transaction Authority or other entrusted bodies.

To cater for electronic delivery of goods such as the downloading of
SUBSTITUTE SHEET (RULE 26) (RO/AU)

SUBSTITUTE SHEET (RULE 26) (RO/AU)

software, digital video, music, or any data, through e-mail or the Internet, the e-mail, Internet or other electronic address is linked to an Address Code representing a real physical address and this linked electronic address is also stored in the publicly readable database 27 thereby enabling protection against fraudulent use.

5 The code for the physical address (the "Address Code") may be constructed in a number of ways, but it is desirable that it be a numeric code of similar dimensions to current credit card numbers and capable of automatic processing by computer software. It is also essential that it have a one-to-one correspondence to actual points on the Earth, these points being actual or potential delivery points for
10 customers. For example, every position on the Earth may be identified by a series of numbers. The Earth has a circumference of approximately 40,000 kms (40,000,000,000 mm) which could be divided into points of longitude spaced 400 mm apart at the equator (less at other latitudes and declining to zero at either pole) and into points of latitude spaced 200 mm apart. Thus at the equator there may be
15 100,000,000 points represented by 8 digits. Furthermore the points of latitude may tally 100,000,000 points also, spaced apart by 200 mm and represented by a further 8 digits. An additional dimension, being altitude or virtual altitude, could be represented by a further 3 digits representing 1000 points at a certain position of latitude and longitude, more than enough for a high-rise apartment or points for
20 post office boxes or other densely spaced addresses. For example, if there were 20 post office boxes located at a certain latitude and longitude, the virtual altitude could be represented by the numbers 1 to 20 indicative of the box number or part thereof. A final digit may be used as a check sum giving a total of 20 digits for the complete Address Code. Thus, a virtual grid covering the entire Earth and
25 corresponding in an unambiguous mathematical way with established points of latitude and longitude, could be constructed with each potential delivery point assigned a unique code. The Address Codes may thus be derived by mathematical calculation from survey data of latitude and longitude. This particular method of constructing Address Codes is by way of example only and it will be apparent to
30 those skilled in the art that other algorithms for uniquely reducing a latitude and longitude for a numerical code may equally serve. An Address Code, once established and assigned to a particular street address, including, if appropriate, a
SUBSTITUTE SHEET (RULE 26) (RO/AU)

particular apartment or post office box, etc. would typically be stored in a securely maintained (for example by TSCs) and publicly readable (for example via the Internet) database, with the database having a cross-correlation to the associated physical and (if applicable) electronic address, so that customers, Issuers, TSCs 5 and merchants can check the Address Code supplied against the physical or electronic address of the customer or vice-versa.

The intent of the establishment of a database of Address Codes is that they could function as a proxy for the identity of the customer representing a point of delivery for goods and services which is intimately linked by prior arrangement to 10 the holder of the account from which payment is requested. As such an unforgeable proxy for identity the Address Code may have a myriad of other uses including routing for postal services and the like, delivery of and billing for, utilities such as electricity, water, telephone, etc., and any other commercial functions where the address for delivery is important. It is worthy of note that the 15 Address Code relates to a particular place and is recorded in the public database 27 the data of which may be independently verified (and is therefore not forgeable provided the database is securely maintained) while the link with a particular Address Code is made by a person on specific request and that link is stored in a secure, private database thus preserving privacy.

20 Figures 4(a) to 4(c) show examples of the database 27 that can be used for maintenance and operation of Address Codes. In Figure 4(a) a user will access the database and if the user knows the Address Code will input this code at 200 to obtain an output latitude and longitude corresponding to the input Address Code at 202. Similarly a known latitude and longitude may be input at 204 to obtain a 25 corresponding output Address Code at 206. This database may be implemented using calculating software and links every unique geographical point on Earth to a unique numerical Address Code or range of Address Codes. The Address Codes are derivable by calculation from longitude and latitude, as previously mentioned, and where the database is published it can be securely maintained by a suitable 30 entrusted body.

In Figure 4(b) a database linking all active Address Codes to a corresponding delivery address, P.O.Box number or

apartment number or similar, is shown. A user knowing the Address Code may input this at 208 to obtain as an output a corresponding street address at 210. Similarly, a user knowing the street address or delivery address may input this at 212 to obtain a corresponding output Address Code at 214. The database can be 5 publicly readable over the Internet 20, is securely maintained and is verifiable by calculation from survey data.

In Figure 4(c) there is shown a further example of a database 27 which links active Address Codes to corresponding electronic addresses for delivery of goods and/or services, for example, e-mail or various files. A user knowing the Address 10 Code may input this at 216 to receive a corresponding electronic address as an output at 218. Similarly, knowledge of the electronic address at 220 may be input to receive or check a corresponding Address Code as an output at 222. Again this database may be publicly readable and securely maintained and amended only by an entrusted authority or body such as the TSCs 24.

15 It is to be noted that personal data is not contained in any of the above public database examples. A Person, whether corporate or individual, may have one or more Address Codes and one or more Persons may share an Address Code (corresponding to a delivery address) although in principle sufficient Address 20 Codes exist for more than one to be assigned to the same street address, therefore making it possible for individuals sharing a delivery address to be assigned distinct Address Codes. The Address Codes however, correspond to addresses rather than persons, at least publicly, and privacy is thereby maintained.

If all of the information is valid and the requested amount is within 25 available limits, the TSCs 24 will obtain or generate from a first storage means, such as database 29 storing a multitude of useable, potential Transaction Codes a Transaction Code which relates only to a particular transaction involving a specific Merchant Code and specific Address Code as requested by the customer and corresponding to a delivery address specified by the customer when originally requesting the remote transaction facilities. This Transaction Code is then 30 transmitted to the Issuer and is also stored in the database 26 of the TSC together with Issuer details, customer account number, Merchant Code, limit amount, time limit (if applicable) and Address Code. An example of the data stored in database

SUBSTITUTE SHEET (RULE 26) (RO/AU)

26 is shown in Figure 6. The database 26 may be maintained by the one or more TSCs and/or the Issuer wherein various responsibilities may be shared or delegated between the TSCs and the Issuer. The database 26 is private and highly secure. The Issuer will in turn transmit this Transaction Code to the customer over a 5 transmitting means, such as the PSTN 14 or the Internet 20 or through ATM connections or other Issuer to customer communications systems. Thus the funds, up to the limit amount for the transaction specified, can be paid only to the merchant specified by the Merchant Code and only from the account or card account that has been specified when setting up the remote transaction facility. At 10 this stage, the transaction has been authorised by the TSCs 24 and the Issuer 22. If for some reason authorisation is denied then the customer must negotiate with their Issuer to come to some agreement as to how the transaction may be authorised.

The customer, now having a Transaction Code, subsequently communicates with the merchant either by way of post, telephone, facsimile, e-mail or through 15 the World Wide Web at the merchant's website. The credit card or debit card number or account number and Passcode are not transmitted to the merchant.

In a preferred implementation, the customer informs the merchant as to the Limit Amount and the Transaction Code. These items represent the authorisation and payment for the transaction so that the merchant can be confident (after getting 20 approval as hereinafter described) that they will receive funds from the customer pertaining to this transaction and the customer will be confident that delivery will be made to the correct address. The merchant will then typically key the amount (up to but not exceeding the Limit Amount), the Transaction Code and the Merchant Code into a terminal which may be their PC 12 or a dedicated terminal 25 (some or all of this may be done automatically by appropriate software), and transmit this information to the TSCs 24 over the PSTN 14 or Internet 20 to obtain approval for the charge. Alternatively, in a manual implementation, the merchant may read this information over the telephone. If the Merchant Code and Transaction Code match those originally supplied by the customer and the amount 30 is not more than the Limit Amount specified by the customer, the TSC will transmit the nominated Address Code of the customer together with an approval code to the merchant. The merchant is now in a position to deliver the goods

SUBSTITUTE SHEET (RULE 26) (RO/AU)

and/or services to the customer after consulting the database 27 to find the physical or electronic address corresponding to the Address Code.

In an alternative implementation, the customer may transmit the nominated Address Code and/or delivery address (physical or electronic), in addition to the Transaction Code and amount, to the merchant. Then when obtaining approval from the TSC the merchant will transmit the Address Code as well as the previously mentioned information to the TSC which will check the Address Code as well as the Merchant Code and amount and will issue an Approval Code only if all supplied codes are correct.

10 The merchant may also check that the supplied Address Code matches the physical or electronic delivery address requested by the customer by consulting the publicly available database 27 mentioned previously.

If the merchant finds the Address Code supplied does not match the delivery address requested, or if in the alternative implementation the TSC rejects the Address Code as not matching one of the registered addresses for use with the account, the merchant will not make delivery until resolution of the mismatch is achieved. The transaction will not proceed and so delivery of goods will not be made to an incorrect address, perhaps requested by a fraudulent user, but only to the correct address of the genuine customer. This would require the cooperation of the merchant to make deliveries only to the legitimate and correct address as specified in the Address Code and it will be the responsibility of the merchant to check, by reference to the publicly accessible database 27 that the Address Code does indeed match the delivery address. Where electronic delivery is required, it is essential that delivery is performed by the merchant after approval for the transaction has occurred and in a separate communication to ensure delivery to a genuine electronic address. The TSCs will be able to consult their secure database 26 and match the Transaction Code, amount, Merchant Code and (optionally) Address Code with those communicated by the merchant. Unless all the codes match, the charge will not be approved and a message denying the charge and perhaps identifying the reason will be transmitted to the merchant. The merchant may then be forced to contact the customer and check that all items of information given by the customer were in fact correct. At this stage, the merchant has not

supplied any goods or services to the customer and no funds have yet been transmitted so no losses have been incurred. If however, the codes do match then the TSCs 24 will inform the merchant either through the Internet or over the PSTN that the charge has been approved and that the transaction is valid and will issue an 5 Approval Code (and in the preferred implementation also the Address Code) to the merchant. The merchant is now in a position to supply the goods or services to the customer at the legitimate address nominated previously by the customer when requesting remote transaction facilities from the Issuer, and may be confident of receiving payment.

10 The merchant is subsequently able to deposit funds for the approved transaction into their Acquirer account either by written summary or electronically through their terminal, either PC 12 or a dedicated terminal. The funds are then transferred from the Issuer (customer's bank) to the Acquirer (merchant's bank) as follows: The merchant supplies the Transaction Code, amount and Merchant 15 Code, together with the Address Code and the Approval Code issued by the TSC on approving the charge, to the Acquirer which supplies these to TSCs 24. The TSCs 24 will supply this data to the Issuer which after checking its records on the Transaction Code, amount, Merchant Code and Address Code will transfer payment back to the Acquirer and the account of the merchant. The details of 20 internal funds and information transfer between financial institutions and TSCs may vary according to existing or future protocols.

The Transaction Code, together with the Address Code authorise one transaction only and the Transaction Code is linked to a particular Merchant Code so that only the holder of that Merchant Code can obtain funds from the customer. 25 Once processed the Transaction Code would cease to have further validity and after a suitable interval could be re-used for an entirely different transaction involving different customers and merchants. If the Transaction Code were formatted in 20 digits similar to an existing credit card number and expiry date it would be large enough to cater for sufficient transactions as well as allow for some 30 basic routing information to assist TSCs in directing verification to the appropriate centres and a check sum to maintain data integrity.

In an allowed variation, the transaction may be specified by the customer to

~~SUBSTITUTE SHEET (RULE 26) (RO/AU)~~
SUBSTITUTE SHEET (RULE 26) (RO/AU)

take into account periodic payments to the merchant for goods or services. An example of such situation is where the customer may not have adequate funds at the time of initiating the transaction but is able to make a series of payments over a period of time. In this situation one Transaction Code, appropriately identified (for 5 example by one digit having a particular value) may be used by the merchant each time a periodical payment is ordered by the customer. Each periodic payment or instalment could be charged by the merchant using the one Transaction Code for all of the transaction up to an authorised limit, thus saving the customer from having to obtain a new Transaction Code for each instalment for the same goods or 10 services. Control of the process remains with the customer in that they would have to authorise the limits of amount and time when requesting the Transaction Code. In another variation, where the customer has established a trustful relationship with a particular merchant, multiple transactions could be pre-authorised based on the one Transaction Code (again appropriately identified). The merchant would then 15 have the Transaction Code and, optionally, the customer's Address Code to use for making claims up to an authorised limit. The procedure followed by the customer for obtaining this semi-permanent Transaction Code (SPTC) would be the same as described above except that this SPTC would be applicable up to an authorised limit and for an authorised time (which might, for example, be up to the expiry 20 date of the card for card accounts) and for a number of transactions involving the same merchant. The trusted merchant therefore retains this SPTC and, optionally, the customer's Address Code and uses them to make any additional charges on request by the customer in the same way as merchants now can do this with credit or debit card numbers held on their files. A particular example is where successive 25 volumes in a series of books are published over a period of time and are supplied by the merchant pursuant to a standing order. The process of the merchant gaining approval for each individual transaction, would, as with existing systems, confirm the availability of funds from the customer's account.

In the event that the merchant's systems were for some reason insecure, no 30 loss would result from the theft of SPTCs kept on file as these would be valid only for transactions between the customer and the holder of the authorised Merchant Code. This may be contrasted with the present situation where credit card

numbers kept on file by merchants may be stolen and used for fraudulent purposes.

A method of enhancing security against merchant fraud may be to allow only merchants with a proven track record to become eligible for SPTCs.

In the event that the customer wishes to cancel a transaction before 5 presentation by the merchant, the customer contacts the Issuer and quotes the Transaction Code and Passcode and requests cancellation. The card or account number is not transmitted and the Issuer after making the appropriate checks would notify TSCs that the Transaction Code was no longer valid. However, if the merchant had already processed the transaction it would not be reversible by this 10 means, but would require the customer to obtain a refund through normal commercial procedures. Any unreasonable level of customer dissatisfaction would result in cancellation of the merchant's facility and Merchant Code by the Acquirer 30 and TSCs 24.

In the event that the customer wishes to change the address for delivery 15 (and Address Code) or other account information they will need to contact the Issuer and undergo checks at least as rigorous as those employed when setting up the remote transaction facility. As this is likely to be an infrequent occurrence it need not be burdensome either to the customer or to the issuing institution.

Shown in Figure 2 is a flow diagram 100 showing the steps involved when 20 a customer applies to their Issuer for remote transaction facilities. First of all at step 102 the customer already having a credit or debit card or suitable account with the issuing financial institution such as a bank, will contact their Issuer to request remote transactions facilities and provide a physical address for delivery of goods as well as optionally an associated electronic address. After performing the 25 necessary checks the Issuer will then issue the customer with, or cause the customer to select a Passcode at step 104 which may require on each occasion when a customer applies for a Transaction Code that they specify a combination of digits out of the total number of digits that make up the Passcode as previously described. The Issuer also issues or records one or more Address Codes, after 30 consulting database 27, wherein one of the Address Codes is required to be nominated by the customer each time they make a Transaction Code request. Subsequently at step 106 the Issuer may transmit the customer's card or account

SUBSTITUTE SHEET (RULE 26) (RO/AU)

number, expiry date and Address Code, stored in the Issuer's database 31, to TSCs 24 to be stored in database 26 for later use in verifying and authorising transactions by the customer.

In Figure 3 there is shown a flow diagram 110 depicting the processes 5 involved when a customer conducts transactions with a merchant and also depicting the processes involving the merchant when they make a claim for payment. At step 120, the customer initiates a remote transaction after contacting a merchant through one of the available channels (by post or mail order, telephone, facsimile, e-mail or World Wide Web) and having selected goods or services that 10 they wish to purchase. The customer will obtain from the merchant an approximate amount for the goods or services requested and their Merchant Code.

At step 122, the customer contacts their Issuer and requests authorisation for payment for the goods or services. The customer is then requested to transmit the limit amount of the transaction, expiry date of their card or facility, the number of 15 their card or account or an agreed reference to it, the Merchant Code, their Passcode or a sub-set of the digits making up their Passcode and their nominated Address Code or an agreed reference to it if more than one Address Code has been registered at step 104. This is usually performed over a relatively secure channel using the PSTN 14 or alternatively where the Internet 20 is used, a suitable 20 protocol such as SSL may be used to encrypt the information that has to be transmitted although encryption of this transmission is not essential. At step 124, the Issuer confirms and validates the card or account number, Address Code and the Passcode, after consulting the Issuer database 31, and transmits the card or account number, Limit Amount, Address Code and the Merchant Code to the 25 TSCs 24 for authorisation. The Merchant Code is used and stored in database 26 so that at a later time when the merchant claims for payment for the transaction, it provides a check as to the identity of the rightful merchant. The TSCs 24 may already have details on the card or account number so that they can make the appropriate checks and authorise the transaction at step 126. If for some reason the 30 transaction is denied, for example, if the customer has extended beyond their credit limit, the customer will be required to negotiate with the Issuer through alternative channels at step 128 to enable the transaction to be processed. For example, the

SUBSTITUTE SHEET (RULE 26) (RO/AU)

SUBSTITUTE SHEET (RULE 26) (RO/AU)

customer may request a greater credit limit to enable them to purchase particular goods or services. The process will then revert back to step 122. If the transaction is authorised by the TSCs 24 , the TSCs 24 will transmit a Transaction Code to the Issuer, after accessing database 29 and storing the Transaction Code in 5 the database 26, at step 130. The Transaction Code may be used for one transaction only or may be a semi-permanent Transaction Code enabling several transactions where the customer has established a trustworthy relationship with a particular merchant, or the Transaction Code may be such as to allow for periodical payments as previously described. At step 132, the Issuer transmits the 10 Transaction Code to the customer for the requested transaction. At step 134, the customer will contact the merchant and disclose to the merchant the Transaction Codes and the Limit Amount. Optionally, the Address Code (or the physical or electronic address) may at this stage also be transmitted by the customer to the merchant to validate a remote transaction request. At step 136, the merchant will 15 then request approval of the particular transaction and transmit to the TSCs 24 an amount not exceeding the Limit Amount, Transaction Code, the Address Code, if supplied, and their Merchant Code. All of this information is stored with the TSCs, in database 26, so that they will be able to make a direct comparison and validate the transaction on that basis at step 137. Shown at Figure 6 is a database 20 maintained by TSCs. In practice the information storage may be shared between Issuer and TSCs according to various protocols but the TSCs will have access to or can request via secure communication channels such information as is required to validate and approve Transaction Codes and the associated merchant and Address. 25 Codes. If for some reason the transaction is denied, the process moves to step 138 where the merchant contacts the customer and checks that all the information provided by the customer to the merchant is in fact correct and to rectify the transaction which will then return to step 134. When the transaction has been approved by the TSCs, the process moves to step 140 and the TSCs transmits to the merchant an approval code and the nominated Address Code. The merchant is 30 then in a position to supply the goods or services to the customer at step 142 after confirming the physical address or electronic address that is linked to the Address Code on the database 27. At step 144 the merchant is able to claim for the amount

SUBSTITUTE SHEET (RULE 26) (RO/AU)

SUBSTITUTE SHEET (RULE 26) (RO/AU)

of the transaction and initiate the transfer of funds from the customer's account to the merchant's account in accordance with the method previously described.

If a customer wishes to change their delivery address it will require the customer to inform the Issuer of such change independently of any individual transaction at which point the Issuer can make rigorous checks as to the correct identity of the customer.

Shown at figure 7 is information 33 required to be stored by the customer in order to use the system. The information is typically stored in a customer database possibly maintained on a PC. Examples include the contact details of the Issuer, the customer identifier or account number and the customer's Passcode and Address Code(s) or references to them. Where computer transactions are used, communication between the customer and Issuer will be implemented using suitable software. Relatively low levels of security of this information are adequate.

The present invention provides a method of conducting financial transactions remotely where no credit or debit card numbers are transmitted between customer or card holder and a merchant. The only relatively secure channel required is that between the customer and the Issuer where the customer informs the Issuer of their credit card or account number, Passcode and delivery address (or Address Code). This can be conducted over a secure channel such as by telephone or by facsimile. The method provides the benefit of having a requirement for two codes to authorise a particular transaction, the Transaction Code and the Address Code, where the Address Code is used to ensure delivery of goods to the legitimate address. The Address Code, by virtue of its being a delivery address belonging only to the legitimate account holder is in effect, the signature of the customer that confirms the authority to approve a particular transaction. An illegitimate user wishing to make any fraudulent transaction would need to know the card or account number and its associated Address Code, together with the customer's Passcode and would need to contact the Issuer through one of the pre-arranged channels at which point any suspicious activity would be more readily detected, could be easily investigated, and, if warranted, issuance of the Transaction Code could be refused. Furthermore, the proceeds of

SUBSTITUTE SHEET (RULE 26) (RO/AU)

SUBSTITUTE SHEET (RULE 26) (RO/AU)

such fraudulent transaction would only be delivered to the legitimate delivery address of the account holder and would therefore be of no value to the fraudulent user.

Once this system is in place, it is envisaged that credit card numbers would 5 no longer be valid for remote transactions and would be replaced by Transaction Codes, which may include semi-permanent codes or codes catering for periodical payments to one merchant, and card numbers would only be valid for local and physical transactions, that is on presentation of the card itself. The system would therefore eliminate the potential for merchant fraud from retained card numbers 10 after physical transactions or fraud from card numbers obtained from discarded transaction slips. Furthermore, only the legitimate holder of a valid Merchant Code could obtain funds for the transaction and only valid Merchant Codes would enable the generation of Transaction Codes. In addition, delivery of the goods will be made only to the legitimate address of the customer, and in the case of an 15 electronic address, this is matched to a registered physical address.

The control of available credit which might be affected by uncompleted transactions is returned to the customer (or account holder) who can cancel an unused authorisation and restore their credit limit.

The system, requires very little new technology to adapt from present 20 systems, does not require encryption, and could take advantage of future improvements in secure communications, personal card readers and/or biometric devices attached to a customer's computer. By employing Address Codes as a proxy for customer identity as described, the security or otherwise of communications would be of little importance as the information is only of value 25 to the legitimate user of the system. The principles involved in the invention described are not reliant on technology of a particular kind and the identifiers employed are universal ones which are not susceptible to technological obsolescence, i.e. a customer will always have an address which, in encoded form, will reliably serve as a substitute for identity in the situation where the customer is 30 not physically present. This independence from technology makes the invention future-proof.

CLAIMS

1. A method of conducting a financial transaction between a customer and a merchant, wherein said customer is remotely located from said merchant and said customer having an account associated with a credit card or debit card or the like from which funds for said transaction will be drawn by said merchant, said merchant having a Merchant Code for use in said transaction, the method comprising the steps of:
 - 10 providing a Transaction Code to said customer for use in said transaction as a substitute for the account number of said customer;
 - 11 establishing an Address Code for said customer that represents a delivery location for goods and/or services provided by said merchant to said customer;
 - 12 wherein in order to authorise said transaction, said customer provides said merchant said Transaction Code such that the account number of said customer is not disclosed to said merchant.
2. A method according to claim 1 further comprising the step of linking said Address Code to a physical address location.
- 20 3. A method according to claim 1 further comprising the step of linking said Address Code to an electronic address that is mapped to a physical address location.
- 25 4. A method according to any one of the previous claims further comprising the step of linking said Merchant Code to said Transaction Code such that said Transaction Code is associated with said Merchant Code in said transaction.
- 30 5. A method according to any one of the previous claims wherein to initiate said transaction said customer requests a Transaction Code from a transaction authority for use in conducting said financial transaction.
6. A method according to claim 5 wherein in order to receive said Transaction

Code said customer supplies to said transaction authority said account number, a Passcode and said Address Code or an agreed reference to said Address Code.

7. A method according to claim 6 wherein said customer further provides to
5 said transaction authority said Merchant Code and a Limit Amount for the transaction, said Limit Amount representing the cost of the goods and/or services that cannot be exceeded.

8. A method according to claim 7 wherein in order to authorise said
10 transaction said customer transmits to said merchant said Limit Amount representing the cost of the goods and/or services.

9. A method according to claim 8 further comprising the step of said
15 merchant, in order to claim funds from the customer for said transaction, transmitting an amount not exceeding said Limit Amount, said Merchant Code and said Transaction Code to said transaction authority.

10. A method according to claim 9 whereupon validating said amount, said
20 Transaction Code and said Merchant Code received from said merchant, said transaction authority transmits to said merchant an Approval Code and said Address Code.

11. A method according to claim 10 further comprising the step of said
25 merchant subsequently verifying that the received Address Code corresponds to said delivery location and thereafter forwarding said goods and/or services to said delivery location.

12. A method according to claim 10 or claim 11 further comprising the step of
30 said merchant using said Approval Code to transfer funds for said transaction from said account of said customer to an account of said merchant.

13. A method according to any one of the previous claims wherein said

SUBSTITUTE SHEET (RULE 26) (RO/AU)

Transaction Code is used for authorising multiple transactions between said customer and said merchant.

14. A method according to any one of the previous claims wherein said
5 Transaction Code is used by said merchant to claim funds of said customer where part payments are made by said customer for said transaction.

15. A method according to claim 13 or claim 14 wherein an Limit Amount is set for said part payments or said multiple transactions.

10 16. A method according to any one of claims 1 to 9 wherein said Address Code or nominated delivery location is transmitted to said merchant by said customer.

15 17. A method of validating a financial transaction between a customer and a merchant, where said customer is remote from said merchant, said method comprising the steps of:

establishing an Address Code for said customer, said Address Code representing a delivery location for goods and/or services provided by said merchant to said customer;

20 matching said Address Code to a physical address of said customer;

providing a data storage means for storing said Address Code and associated physical address;

25 wherein use of said Address Code in said financial transaction ensures that delivery of said goods and/or services is to the address nominated by said customer and thereby validates said transaction.

30 18. A method according to claim 17 further comprising the step of linking said Address Code to an electronic address mapped to said physical address in situations where said goods and/or services are transmitted electronically to said customer.

19. A method according to claim 17 or claim 18 further comprising the step of

SUBSTITUTE SHEET (RULE 26) (RO/AU)

SUBSTITUTE SHEET (RULE 26) (RO/AU)

said customer requesting a Transaction Code for use in said transaction as a substitute for a number of an account of said customer from which funds are drawn by said merchant.

5 20. A method according to claim 19 further comprising the step of linking said Transaction Code to a Merchant Code, said Merchant Code identifying said merchant.

10 21. A method according to claim 19 or claim 20 further comprising the step of said customer providing a transaction authority or an issuing institution with the account number of said customer, a Passcode and said Address Code in order to receive said Transaction Code.

15 22. A method according to claim 21 further comprising the step of said customer providing said transaction authority or said issuing institution said Merchant Code and a Limit Amount for the transaction, said Limit Amount representing the cost of the goods and/or services that cannot be exceeded.

20 23. A method according to claim 22 further comprising the step of said customer transmitting to said merchant said Transaction Code, said Limit Amount and a nominated delivery address in order to authorise the transaction.

25 24. A method according to claim 23 further comprising the step of said merchant, in order to claim funds from the customer for said transaction, transmitting an amount not exceeding said Limit Amount, said Merchant Code and said Transaction Code to said transaction authority.

30 25. A method according to claim 24 whereupon validating said amount, said Transaction Code and said Merchant Code received from said merchant, said transaction authority transmits to said merchant an Approval Code and said Address Code.

26. A method according to claim 25 further comprising the step of said merchant subsequently verifying that the received Address Code corresponds to said delivery location and thereafter forwarding said goods and/or services to said delivery address.

5

27. A system for conducting a financial transaction between a customer and a merchant, wherein said customer is remotely located from said merchant and said customer having an account associated with a credit card or debit card or the like from which funds for said transaction will be drawn by said merchant, said merchant having a Merchant Code for use in said transaction, the system comprising:

a first storage means for storing a Transaction Code for use in said transaction, said Transaction Code being a substitute for the number of said account of said customer;

15 means for transmitting said Transaction Code to said customer in response to a request by said customer for approval for said transaction; and

a second storage means for storing an Address Code, said Address Code being linked to a delivery location nominated by said customer where goods and/or services provided by said merchant as part of said transaction are to be delivered;

20 wherein in order to authorise said transaction, said customer provides said merchant said Transaction Code such that said account number of said customer is not disclosed to said merchant.

28. A system according to claim 27 wherein said delivery location is a physical
25 address.

29. A system according to claim 27 wherein said delivery location is an electronic address mapped to a physical address.

30 30. A system according to any one of claims 27 to 29 wherein said Transaction Code is linked to said Merchant Code.

31. A system according to claim 30 wherein said request for authorisation for said transaction is sent to a transaction authority, said transaction authority accessing said first storage means in order to retrieve or generate said Transaction Code and thereafter delivering said Transaction Code to said customer.

5

32. A system according to any one of claims 27 to 30 wherein prior to receiving said Transaction Code said customer supplies said transaction authority or an issuing organisation with said customer account number, a Passcode and said Address Code obtained from said second storage means.

10

33. A system according to claim 32 wherein said customer further provides to said transaction authority or said issuing organisation said Merchant Code and a Limit Amount for the transaction, said Limit Amount representing the cost of the goods and/or services that cannot be exceeded.

15

34. A system according to claim 33 wherein after receiving said Transaction Code said customer sends to said merchant a nominated delivery address and said Limit Amount representing the cost of the goods and/or services as part of the authorisation of said transaction.

20

35. A system according to claim 34 wherein in order to claim funds from the customer for said transaction, said merchant transmits to said transaction authority an amount not exceeding the Limit Amount, said Transaction Code and said Merchant Code.

25

36. A system according to claim 35 whereupon validating said amount, said Transaction Code and said Merchant Code received from said merchant, said transaction authority transmits to said merchant an Approval Code and said Address Code for said customer.

30

37. A system according to claim 36 wherein said merchant accesses said second storage means to verify that the received Address Code corresponds to the

nominated delivery address of said customer.

38. A system according to any one of claims 27 to 37 wherein said second storage means is a database that is publicly accessible and stores Address Codes 5 and corresponding physical addresses.

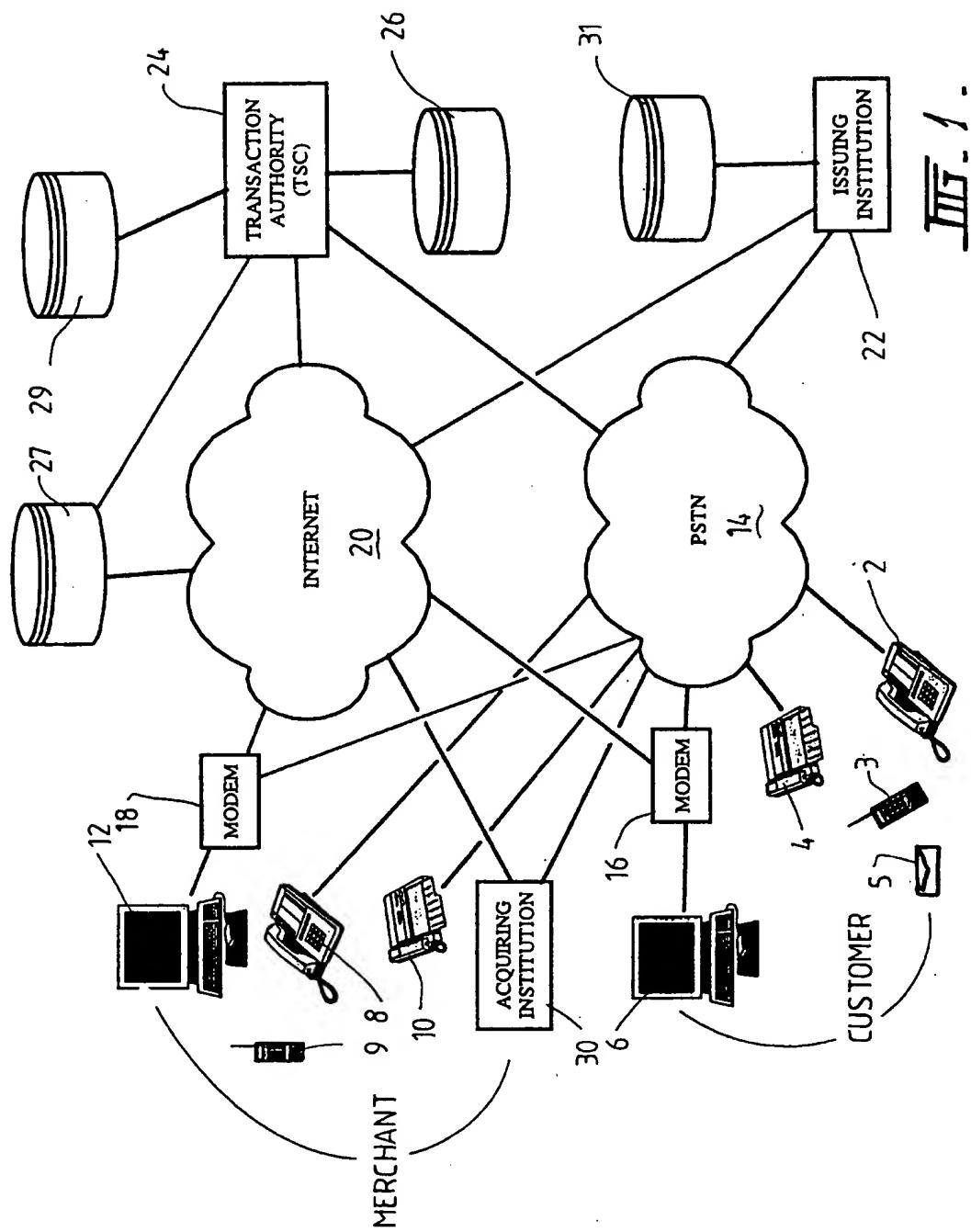
39. A system according to any one of claims 27 to 38 wherein said system further comprises a communications network through which one or more transmissions of data is made between said customer, said merchant and said 10 transaction authority.

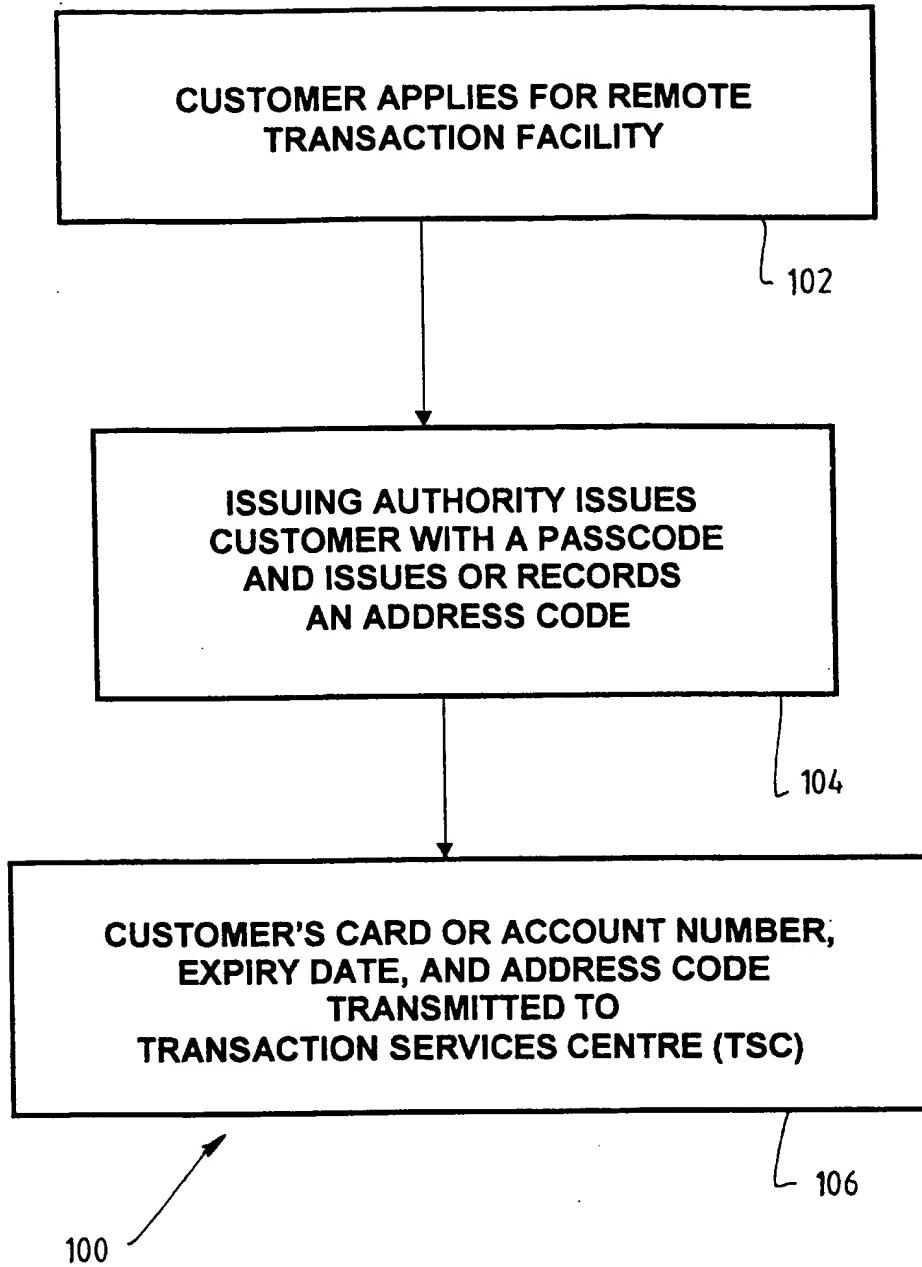
40. A method of ensuring correct delivery of goods and/or services to a customer from a merchant as a result of a remote transaction between said customer and said merchant, said method comprising the steps of:

15 establishing a storage means for storing one or more Address Codes, wherein each stored Address Code represents a delivery location for receipt of said goods and/or services;

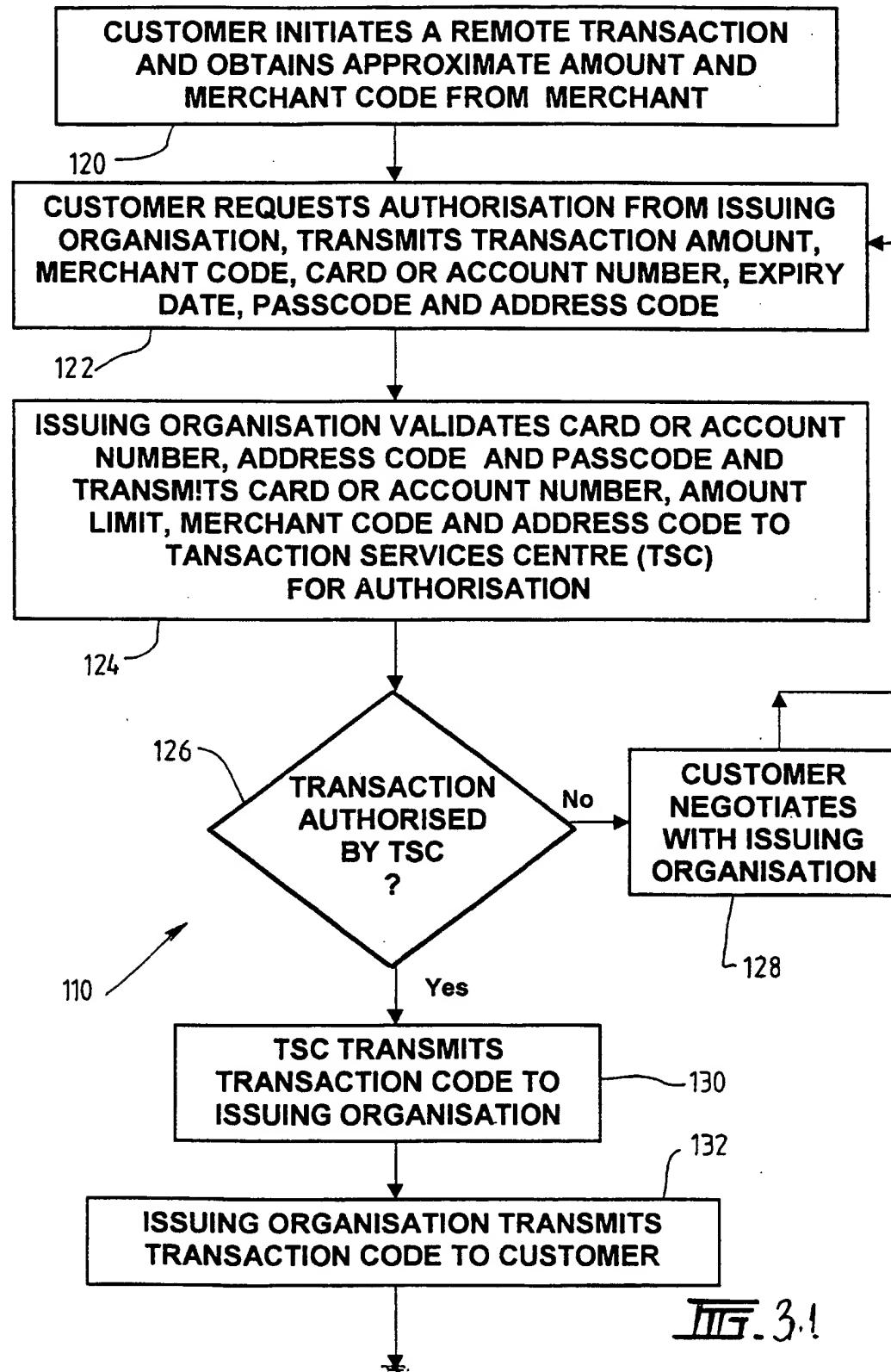
matching said Address Codes to respective physical addresses in said storage means; and

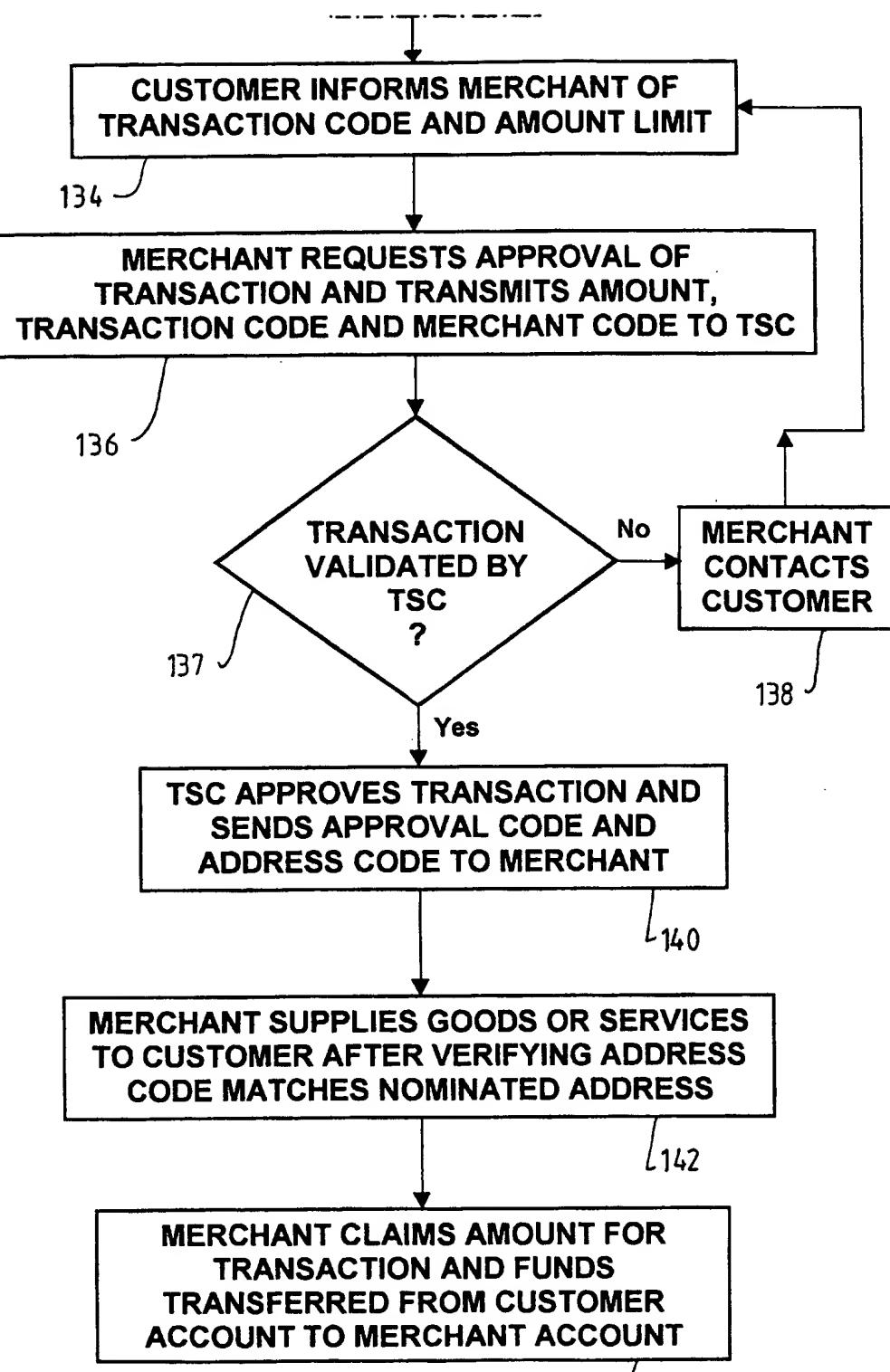
20 accessing said storage means in order to retrieve a corresponding delivery location on entering an Address Code or in order to retrieve an Address Code corresponding to an entered delivery location.





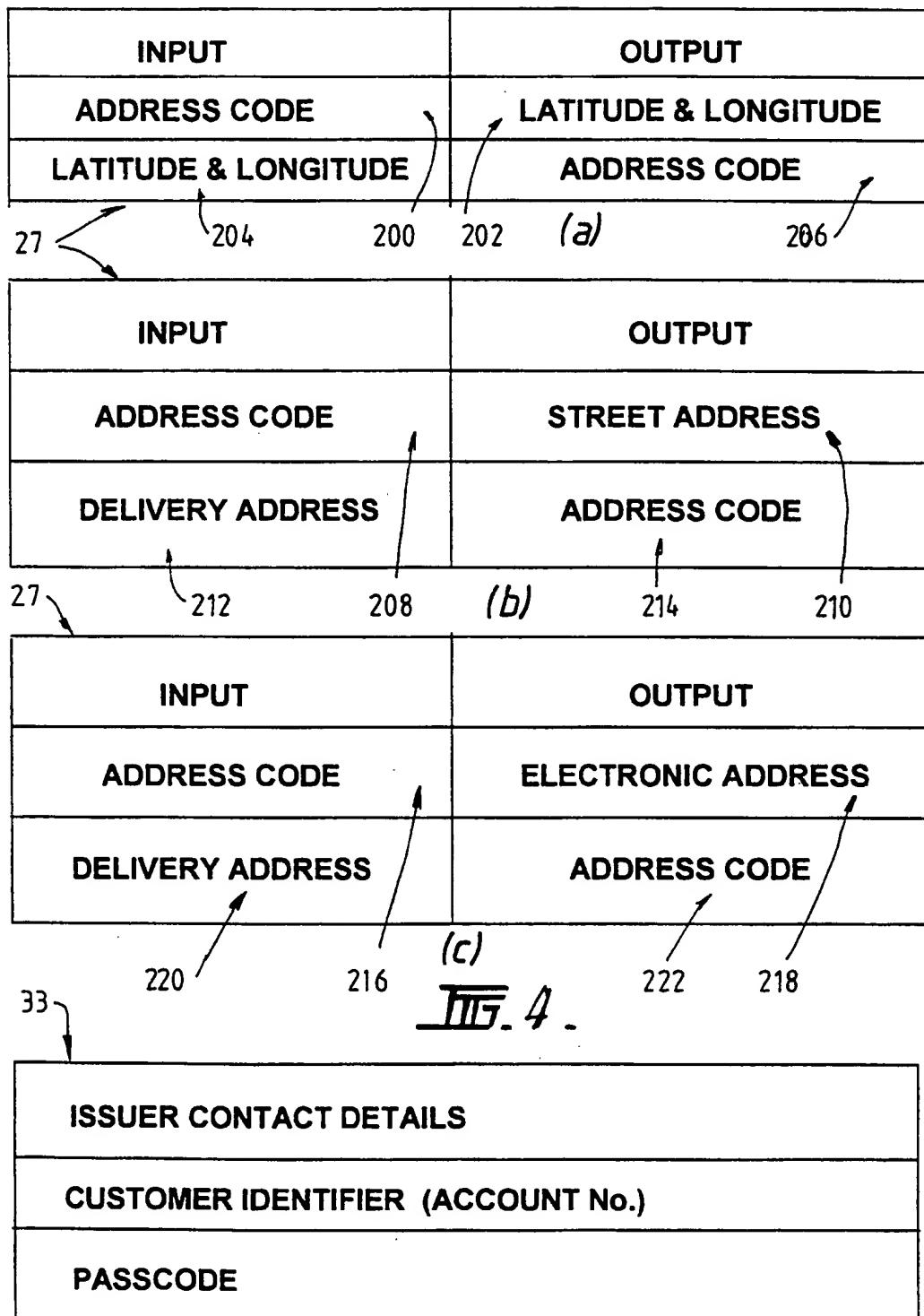
III. 2.





III-32-

SUBSTITUTE SHEET (Rule 26) (RO/AU)

FIG. 4.

SUBSTITUTE SHEET (RULE 26) (RO/AU)

| | | |
|--|---|--------|
| CUSTOMER NAME AND BILLING ADDRESS | | |
| ACCOUNT NUMBER AND INTERNAL IDENTIFIERS | | |
| ACCOUNT STATUS AND BALANCE | | |
| EXPIRY DATE | | |
| CREDIT LIMITS | | |
| PASSCODE INFORMATION | | |
| ADDRESS CODES | 0 | CODE 1 |
| 31 | 1 | CODE 2 |
| 32 | 2 | CODE 3 |

31 III-5- 32 III-6-

26

| |
|--|
| TRANSACTION CODE |
| TRANSACTION TYPE |
| ISSUER DETAILS |
| CUSTOMER IDENTIFIER (ACCOUNT No.) |
| MERCHANT CODE |
| LIMIT AMOUNT |
| TIME LIMIT |
| ADDRESS CODE |

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU 99/00536

| | | |
|--|--|--|
| A. CLASSIFICATION OF SUBJECT MATTER | | |
| Int Cl ⁶ : G06F 17/60 | | |
| According to International Patent Classification (IPC) or to both national classification and IPC | | |
| B. FIELDS SEARCHED | | |
| Minimum documentation searched (classification system followed by classification symbols) G06F | | |
| Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Internet see extra sheet | | |
| Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) WPAT See extra sheet | | |
| C. DOCUMENTS CONSIDERED TO BE RELEVANT | | |
| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
| X | US, A, 5292004 (Cesarini) 8 March 1994 | 40 |
| A | US, A, 5629982 (Micali) 13 May 1997 | |
| A | US, A, 5557518 (Rosen) 17 September 1996 | |
| <input type="checkbox"/> Further documents are listed in the continuation of Box C | | <input checked="" type="checkbox"/> See patent family annex |
| <ul style="list-style-type: none"> * Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed | | <ul style="list-style-type: none"> "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family |
| Date of the actual completion of the international search 4 August 1999 | Date of mailing of the international search report 10 AUG 1999 | |
| Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200 WODEN ACT 2606 AUSTRALIA Facsimile No.: (02) 6285 3929 | Authorized officer Stephen Lee Telephone No.: (02) 6283 2205 | |

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU 99/00536**Box****WPAT**

ESCROW: OR (TRANSACT: OR TRAD: OR BUY: OR SELL:) AND (MERCHANT: OR CUSTOMER:) AND (TRUST: (W) AGENT# OR THIRD) OR (TRANSACT: OR TRAD: OR BUY: OR SELL:) AND (MERCHANT: OR CUSTOMER:) AND OPEN AND (ADDRESS OR LOCATION OR PLACE OR VISA OR MASTERCARD# OR CREDIT (W) CARD# OR BANKCARD#) OR ((VALID: OR AUTHENTIC: OR CONFIRM: OR AUTHORI) AND ADDRESS: AND (TRANSACT: OR FINANC:)) AND (GOODS OR SERVICE# OR COMMODIT: OR BUY: OR SELL: OR TRAD: OR MERCHAN: OR VENDOR# OR SHOP: OR RETAIL: OR WHOLESALE:) OR (ADDRESS: AND (GOODS OR SERVICE# OR COMMODIT:) AND (BUY: OR SELL: OR TRAD:) AND (DELIVER: OR POST: OR MAIL: OR CONSIGN: OR FREIGHT: OR SEND:))

USPTO

((ESCROW AND TRANSACT\$) AND ((CREDIT OR VISA) OR MASTERCARD)) ANDNOT COIN
(("POSTAL SYSTEM" AND (COORDINATES OR "ADDRESS CODE"))
("POSTAL ADDRESS" AND COORDINATES))

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/AU 99/00536

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

| Patent Document Cited in Search Report | | | Patent Family Member | | | | |
|--|---------|----|----------------------|----|----------|----|----------|
| US | 5292004 | AU | 30472/89 | DK | 4863/89 | EP | 327472 |
| | | FR | 2626504 | MC | 2059 | NO | 893910 |
| | | WO | 8907018 | | | | |
| US | 5629982 | CA | 2215908 | EP | 815671 | WO | 9629795 |
| | | WO | 9806198 | US | 5553145 | US | 5629982 |
| | | US | 5666420 | EP | 917781 | | |
| US | 5557518 | AU | 21058/95 | AU | 52835/98 | AU | 52836/98 |
| | | AU | 52837/98 | AU | 52838/98 | BR | 9507107 |
| | | CA | 2184380 | CN | 1147875 | CZ | 9602513 |
| | | EP | 758474 | FI | 964032 | HU | 76463 |
| | | NO | 964538 | NZ | 283103 | NZ | 329065 |
| | | NZ | 329066 | NZ | 329067 | NZ | 329068 |
| | | PL | 317026 | SI | 9520039 | SK | 1176/96 |
| | | WO | 9530211 | US | 5799087 | US | 5621797 |
| | | US | 5642419 | US | 5703949 | US | 5878139 |
| | | AU | 55615/96 | CA | 2218612 | CN | 1185851 |
| | | CZ | 9703323 | EP | 823105 | NO | 974835 |
| | | NZ | 306918 | PL | 323007 | SI | 9620055 |
| | | SK | 1426/97 | WO | 9633476 | WO | 9633476 |

END OF ANNEX